STATE OF MONTANA
DEPARTMENT OF CORRECTIONS
POLICY DIRECTIVE

Policy No. DOC 1.7.6	Subject: **UNLAWFUL USE OF IT RESOURCES**
Chapter 1: ADMINISTRATION AND MANAGEMENT	Page 1 of 4
Section 7: Information Systems	Effective Date: Dec. 1, 1996
Signature: /s/ Mike Batista, Director	Revised: 05/10/2016

I. POLICY

The Montana Department of Corrections requires all state-owned Information Technology (IT) resource equipment or software to be operated lawfully and in compliance with all applicable state statutes.

II. APPLICABILITY

All divisions, facilities, and programs Department-owned and contracted, as specified in the contract.

III. DEFINITIONS

Computer Use – As used in *45-6-311, MCA*, the term "obtain the use of" means to instruct, communicate with, store data in, retrieve data from, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, or computer network or to cause another to instruct, communicate with, store data in, retrieve data from, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, or computer network.

Information Technology (IT) Resource – Any computer system, including but not limited to, computers, servers, printers, smartphones, tablets, laptops, and networks.

Malicious Software – A dangerous computer program with the characteristic feature of being able to generate copies of itself, and thereby spread. Additionally, most Malicious Software has a destructive payload that activates under certain conditions.

Virtual Private Network (VPN) – A network that is constructed by creating a tunnel between a public network, usually the Internet, to connect to a private network, such as a company's internal network.

IV. DEPARTMENT DIRECTIVES

A. General Prohibitions

1. A person commits the offense of unlawful use of an IT resource if they knowingly or purposely:
   a. obtain the use of any IT resource without consent of the owner;
   b. alter or destroy or cause another to alter or destroy an IT resource without the consent of the owner; or

c. obtain the use of, alter, an IT resource, or any part thereof as part of a deception for the purpose of obtaining money, property, information, or computer services from the owner of the computer, computer system, computer network, or part thereof or from any other person.

B. Malicious Software Introduction

1. Users will not intentionally introduce Malicious Software into a state IT resource.

C. Prohibited Uses of State IT Resources

1. Using state IT resources to create, access, download, or disperse derogatory, racially offensive, sexually offensive, harassing, threatening, or discriminatory materials.

2. Downloading, installing, or running security programs or utilities, which reveal or could be used to reveal weaknesses in the security of the state's IT resources, unless your job specifically requires it and it has been approved by the Network Support Bureau Chief or CIO.

3. Attempting to modify, install, or remove state IT equipment, software, or peripherals without proper authorization; including installing any hardware, software, or non-approved external storage device on state-owned IT resources.

4. Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the state, i.e., if you abuse the networks to which the state has access or the computers at other sites connected to those networks, the state will treat this matter as an abuse of your computing privileges.

5. Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations or sharing of personal usernames or passwords for state devices, networks, application or information in accordance with *DOC Policy 1.7.7 Computer Security*.

6. The use of IT resources, User IDs, or IT resource data for purposes other than those for which they were intended or authorized.

7. Sending fraudulent e-mail, breaking into another user's e-mailbox, or unauthorized personnel reading someone else's e-mail without his/her permission.

8. Sending any fraudulent electronic transmission including, but not limited to, fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorization of purchase requisitions or journal vouchers.

10. Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.

11. Taking advantage of another user's naiveté or negligence to gain access to any User ID, data, software, or file that is not your own and for which you have not received explicit authorization to access.

12. Physically interfering with other users' access to the state's computing facilities.

13. Encroaching on or disrupting others' use of the state's shared network resources by creating unnecessary network traffic, e.g., playing games; wasting computer time, connect time, disk space, or other resources; modifying system facilities, operating systems, or disk partitions without authorization; attempting to crash or tie up a state computer; damaging or vandalizing state computing facilities, equipment, software, or computer files.

14. Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.

15. Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission.

16. Knowingly transferring or allowing to be transferred to, from or within the agency, textual or graphical material commonly considered to be child pornography or obscene as defined in *45-8-201, MCA*.

17. Any use for private or commercial profit.

18. Any use for product advertisement or political lobbying.

19. Downloading any confidential or personally identifiable information to any removable storage media that is neither Department-owned nor encrypted.

20. Sharing, giving, or selling Department owned confidential or personally identifiable information with anyone outside of the agency without explicit permission.

21. Use of personal email or unapproved cloud service for transmittal or receipt of Department data.

22. Utilizing VPN services to connect to state networks and resources from personally owned computing devices.

D. Reporting Unlawful Use

1. Users will report unlawful use and other security violations to their immediate supervisor, to local personnel responsible for local network policy enforcement, or to personnel responsible for the security and enforcement of network policies where the violation originated.

2. The Office of Human Resources will report all employee suspensions, resignations, and terminations to the IT security officer as soon as the event takes place. The security officer will suspend the employee’s accounts, thereby preserving evidence for investigation or to prevent malice.

E. Disciplinary Action

1. If, following an investigation, it is determined an employee has violated this policy, immediate termination of network and system access may result.

2. Violators may be subject to disciplinary action up to and including termination under *DOC Policy 1.3.2 Employee Performance and Conduct.* Further, in some cases the severity of the violation may mandate that it be reported to the state's cyber security officer and the state's CIO. Once the reported violation reaches this level, it may involve the attorney general and legislative auditor's office.

F. Legal Action

1. In the event that a Department employee is believed to have been involved in the unlawful use of an IT resource, the Department will pursue an investigation in accordance with *DOC Policy 3.1.19 Investigations*.

V. CLOSING

Questions concerning this policy should be directed to the Chief Information Officer or the IT Policy and Strategic Planning Officer.

VI. REFERENCES

A. 2-15-114, MCA; 2-17-534, MCA; 45-6-310, MCA; 45-6-311, MCA; 45-8-201, MCA
B. 1-0243.40; Montana Operations Manual
C. DOC Policies 1.3.2 Employee Performance and Conduct; 3.1.19 Investigations

VII. ATTACHMENTS

None